

Commonwealth of Virginia Data Trust Member Agreement

The Commonwealth of Virginia Data Trust Member Agreement (the "Agreement") is entered into on _____, 20____ ("Effective Date") by and between the undersigned (hereinafter referred to individually as "Data Trust Member" and collectively as "Data Trust Members"), and the Chief Data Officer for the Commonwealth of Virginia ("Trustee"), on behalf of the Virginia Commonwealth Data Trust ("Data Trust"). Data Trust Member and the Trustee may each individually be referred to herein as a "Party" and collectively as the "Parties."

RECITALS

WHEREAS, the Data Trust Members desire to create and support the Data Trust to achieve defined Shared Goals and enable the Approved Projects and Allowable Uses ("Goals, Projects, and Uses") as further detailed in Exhibit A attached hereto and updated and maintained electronically in the Data Trust Goals, Approved Projects, and Allowable Uses Registry;

WHEREAS, the Data Trust desires to establish, maintain and enforce a set of standards for the mutual benefit of Data Trust Members that will promote the free flow and exchange of information between and amongst the Data Trust Members in a secure electronic environment with the assurance that all such information will be used for lawful purposes;

WHEREAS, the Data Trust Members are organizations that oversee and conduct, on their own behalf and/or through the Commonwealth of Virginia Data Governance Council and/or Executive Data Board, electronic transactions or exchanges of information among groups of persons or organizations, that (i) have the technical ability to electronically transact data on their own behalf or on behalf of their Data Trust Member; (ii) have the organizational infrastructure and legal authority to comply with the obligations in this Agreement and to require their Data Trust Member to comply with applicable requirements in this Agreement; and (iii) have each individually accepted the Agreement as a Data Trust Member;

WHEREAS, each Data Trust Member shall grant ongoing access to or provide Data Trust Member-Contributed Data Resources (as defined below), detailed in Exhibit B attached hereto and maintained on the Data Trust electronic metadata registry, for the Trust to realize the Goals, Projects and Allowable Uses;

WHEREAS, as a condition of transacting data with other Data Trust Members, each Data Trust Member shall enter into this Agreement and has agreed to do so by executing this Agreement;

NOW, THEREFORE, in consideration of the mutual covenants herein contained, the Parties hereto hereby agree as follows:

I. DEFINITIONS

A. In this agreement:

1. **“Data Governance Council”** shall mean the decision-making body, consisting of Employees of Data Trust Members that are state agencies selected by the Executive Data Board, which ensures that the development and deployment of the data trust adheres to the data, technical, and acceptable use specifications outlined in exhibits attached hereto, in addition to managing, monitoring, and sustaining the data trust.
2. **“Data Governance Council Representative”** shall mean the individual employee of a state agency Data Trust Member selected by the Executive Data Board to the Data Governance Council.
3. **“Data Trust”** shall mean the Trustee, Data Trust Member, and other Data Trust Members which collectively form the Data Trust as constituted in this Data Trust Agreement.
4. **“Data Trust Member”** shall mean an organization that has been approved to participate in the data trust and being a party to the Data Trust Agreement. Data Trust Members may include private companies, non-profit organizations, philanthropic and governmental entities, and community and/or advocacy groups as determined and approved by the Trustee.
5. **“Data Trust Member-Contributed Data Resources”** shall mean any data owned by or stewarded over by Data Trust Member or other Data Trust Members provided to the Trustee for use by the Data Trust, designated as Tier 0, Tier 1, Tier 2 or Tier 3 data, and described in Exhibit B or on the Data Trust electronic metadata registry. No Tier 4 data shall be knowingly incorporated into the Data Trust.
6. **“Data Trust Member-Owned Data Resource”** shall mean any data owned by or stewarded over by Data Trust Member or other Data Trust Members.
7. **“Data Trust Access Hub”** shall mean the electronic portal providing approved Data Trust User access to Trust-managed data resources, as outlined in an approved Data Sharing Agreement between the Trustee and the Third-Party User.
8. **“Data Trust Technical Infrastructure”** shall mean any legal agreements, electronic registries, computer code or other technology used to support, maintain, and govern the Data Trust, its Data Trust Member-contributed Data Resources, and Trust-managed Data Resources. This may include, but not limited to, extract, transform, and load (ETL) scripts, databases, distributed ledgers, web applications, algorithms, authorization protocols, application programming interfaces (APIs), and compliance monitoring services.

9. **“Data Trust User”** shall mean any entity or individual that has expressly received permission from the Trustee and appropriate Data Trust Member to use any of the data trust-managed resources for specified purposes.
10. **“Executive Data Board”** shall mean the board consisting of executive leadership, or their designees, from executive branch agencies engaged in data sharing and analytics projects; chaired by the Chief Data Officer.
11. **“Tier 0 Data”** shall mean data or information this is neither sensitive nor proprietary intended for public access provided on an ongoing basis or as a one-time transfer to Trustee by Data Trust Member for use by Data Trust under this Agreement as detailed in Exhibit B attached hereto or subsequently contributed by Data Trust Member detailed in the Data Trust electronic metadata registry.
12. **“Tier 1 Data”** shall mean data that is not protected from public disclosure or subject to withholding under any law, regulation, or contract. Nevertheless, publication of the dataset on the public Internet and exposure to search engines would: have the potential to jeopardize the safety, privacy, or security of a person who may be identified through use of the data; requires subjective redaction to classify the data as Tier 0 data; impose an undue financial or administrative burden on the Data Trust Member; or expose the Trustee or Data Trust Member to litigation or liability.
13. **“Tier 2 Data”** shall mean sensitive or proprietary information intended for access or release only on a 'need-to-know' basis, including personal information not otherwise classified as Tier 0 or 1, and data protected or restricted by contract, grant, or other agreement terms and conditions provided on an ongoing basis or as a one-time transfer to Trustee by Data Trust Member for use by Data Trust under this Agreement as detailed in Exhibit B attached hereto or subsequently contributed by Data Trust Member and detailed in the Data Trust electronic metadata registry.
14. **“Tier 3 Data”** shall mean sensitive or proprietary information and data elements with a statutory requirement under Data Trust Member's relevant state and federal laws for notification to affected parties in case of a confidentiality breach (e.g. Social Security Number, driver's license number, financial account numbers, personal medical information, etc.) provided on an ongoing basis or as a one-time transfer to Trustee by Data Trust Member for use by Data Trust under this Agreement as detailed in Exhibit B attached hereto or subsequently contributed by Data Trust Member and detailed in the Data Trust electronic metadata registry. Examples of Tier 3 Data may include, but not limited to: Attorney-Client Privileged; Criminal Justice Information; Critical Infrastructure Information; Family Educational Rights and Privacy Act (FERPA); Federal or State Tax Information; or Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA).

15. **“Tier 4 Data”** shall mean sensitive or proprietary data where the unauthorized disclosure could potentially cause major damage or injury, including death, to entities or individuals identified in the information, or otherwise significantly impair the ability of the Data Trust Member to perform its statutory functions. Tier 4 Data includes any dataset designated by a federal agency at the level “Confidential” or higher under the federal government’s system for marking classified information.
16. **“Trust-managed Data Resource”** shall be any data resource, including transformed data, generated by the combination of one or more Data Trust Member-contributed Data Resources and managed on behalf of the Trust by the Trustee in support of the agreed upon goals of the Trust, or one or more of the Approved Projects and Uses.
17. **“Trustee”** shall mean the Chief Data Officer of the Commonwealth of Virginia.

II. GOVERNANCE OF THE DATA TRUST

A. To support the Data Trust and its Data Trust Members, there shall be an Executive Data Board and a Data Governance Council.

B. Executive Data Board

1. Composition

- a. Executive leadership, or their designees, from Data Trust Members that are Executive Branch agencies engaged in data sharing and analytics projects.
- b. Data Trust Members, or their designees, selected by the Trustee.

2. Responsibilities

- a. Translate the Commonwealth's data-driven policy goals and objectives to agency performance targets.
- b. Allocate appropriate agency resources to support data governance, sharing, and analytics initiatives.
- c. Provide to the Commonwealth of Virginia Data Commission any reports on the Board's recommendations and work as required by the Commonwealth of Virginia Data Commission.

3. Executive Data Board Chair

- a. The Executive Data Board shall be chaired by the Trustee or the Trustee's designated representative.

4. Executive Data Board Meetings

- a. The Trustee shall have the authority to convene the Executive Data Board.

C. Data Governance Council

1. Composition

- a. State agency employees of Data Trust Members selected by the Executive Data Board

2. Responsibilities

- a. Liaise between state agency operations and the Trustee
- b. Advise the Trustee on technology, policy, and governance strategies
- c. Administer data governance policies, standards, and best practices as set by the Board
- d. Oversee data sharing and analytics projects
- e. Review open data assets
- f. Provide to the Executive Data Board any reports on the Data Governance Council's recommendations and work as required by the Executive Data Board

- g. Develop necessary policies, privacy and ethical standards for Trust-managed Data Resources
 - h. Monitor the sharing of Data Trust Member-Contributed Data Resources
 - i. Review and approve new Trust-managed Data Resources
 - j. Conduct any other business the Trustee deems necessary for Data Trust governance
3. Data Governance Council Chair
- a. The Data Governance Council shall be chaired by the Trustee or the Trustee's designated representative.
 - b. The Data Governance Council Chair is responsible for scheduling meetings.
 - c. Data Governance Council Chair shall create and maintain an electronic registry of all Governance Council representatives.
 - d. Data Governance Council Chair shall create and maintain an electronic registry of all meeting minutes including Governance Council decisions.
4. Data Governance Council Meetings
- a. Meetings for the Data Governance Council shall occur at a minimum of once a quarter, or more frequently if determined by the Data Governance Council Chair.
 - b. Data Governance Council may invite data stewards or subject matter experts to attend meetings in order to provide substantive, technical, and/or contextual expertise for the purposes of discussion.
 - c. Unless otherwise stated, all decisions, approvals and actions taken shall be through a majority vote (50%+1) of the Data Governance Council Representatives present and voting yea or nay at a meeting. Each Data Governance Council Representative, including the Chair, has one equal vote.
 - d. Data Governance Council Representatives must be notified of an upcoming vote at least 5 business days prior to the scheduled meeting.
 - e. Data Governance Council Representatives may temporarily delegate their voting rights to any other individual or Data Governance Council representative by informing the Data Governance Council Chair in writing, 24 hours in advance of any vote that they are delegating their voting rights and to whom the voting rights are to be delegated.

III. DATA TRUST MEMBER RESPONSIBILITIES

- A. It is the Data Trust Member's responsibility to determine the Data Trust Member-contributed Data Resource type, amount, format and content. Data Trust Member agrees to clearly identify and label data provided to the Data Trust hereunder as Tier 0, Tier 1, Tier 2, or Tier 3 data in Exhibit B. Data Trust Member agrees not to provide Tier 4 Data to the Data Trust. From information provided in Exhibit B, Trustee will create an electronic registry of Data Trust Member-contributed data resources. Upon creation of such registry, Data Trust Member agrees to maintain and update data and their classifications therein.
- B. Data Trust Member shall be responsible for obtaining all necessary consents and otherwise complying with all applicable laws and other rules and regulations prior to sharing Tier 1, Tier 2 or Tier 3 data with Trustee for use by the Data Trust.
- C. Data Trust Member represents and warrants that they have secured all necessary approvals from any third parties (if applicable) and has the legal right to provide Trustee any and all data in acting on behalf of the Data Trust for the purposes contemplated by this agreement.
- D. Each Data Trust Member shall require that all of its employees, agents or contractors transact data only in accordance with the terms and conditions of this Agreement, including without limitation those governing the use, confidentiality, privacy, and security of the data. Each Data Trust Member shall discipline appropriately any of its employees, agents or contractors, or take appropriate contractual action with respect to employees, agents or contractors, who fail to act in accordance with the terms and conditions of this Agreement relating to the privacy and security of message content, in accordance with Data Trust Member's employee disciplinary policies and procedures and its contractor and vendor policies and contracts, respectively.
- E. Data Trust Member shall transmit, have access to, and have the ability to request removal at any time, any or all data the Data Trust Member-Contributed Data Resources to the Trust through the Data Trust Technical Infrastructure. Removal of Data Trust Member-Contributed Data Resources will occur within fifteen days of receipt of removal request.
- F. Data Trust Member shall have the ability to grant, change, or revoke access and use of Tier 0, Tier 1, Tier 2 or Tier 3 data at any time for one or more of the approved projects and uses outlined in Exhibit A attached to this agreement. Access may be granted, changed, or revoked at the field, row, or element level and on a user-by-user basis for Tier 1, Tier 2 or Tier 3 data.
- G. Data Trust Members may add to Tier 0, Tier 1, Tier 2 or Tier 3 data shared with the Trustee for use by the Data Trust at any time by updating the online registry of Data Trust Member-Contributed Data Resources in Exhibit B, and by connecting the new data to the Data Trust Technical Infrastructure or by requesting that the Trustee facilitate the connection through automated data pipelines.

- H. Data Trust Member acknowledges and agrees that their Tier 0, Tier 1, Tier 2 or Tier 3 data may be combined with data of other Data Trust Members. All copies of Tier 0, Tier 1, Tier 2, or Tier 3 data provided by Data Trust Member to the Data Trust will be stored, maintained, and monitored using the secure Data Trust Technical Infrastructure detailed in Exhibit E and managed by Trustee on behalf of the Data Trust and its Members. Data Trust Member shall be able to access the complete audit log of all access and use of Tier 0, Tier 1, Tier 2 and Tier 3 data stored on Data Trust Technical Infrastructure at any time through Data Trust Member's electronic portal.
- I. Data Trust Member hereby grants to the Executive Data Board, the Data Governance Council and the Trustee, the right to provide oversight, facilitation and support for the Data Trust Members by conducting activities including, but not limited to, the Responsibilities identified in this Agreement.

IV. TRUSTEE RESPONSIBILITIES

- A. Trustee is responsible for providing the necessary technical and organizational infrastructure to support the creation, use, and maintenance of the Data Trust and ensure all Data Trust Members or Data Trust users are in compliance with the terms and conditions of their agreement(s).
- B. Trustee is responsible for updating the Exhibits of this agreement attached hereto in accordance with approved changes provided by Data Trust Member.
- C. If public access of Tier 0 data is listed as an Approved Use in Exhibit A, once Tier 0 data is contributed by any Data Trust Member, Trustee shall have the right to immediately make Tier 0 Data publicly available as approved and specified therein.
- D. Trustee agrees to keep all Tier 1, Tier 2 and Tier 3 Data Trust Member-Contributed Data Resources confidential and only disclose them to employees, affiliates, contractors or agents who need access in order to meet Trustee's obligations and requirements for Data Trust Members and the Data Trust for the purposes contemplated by this Agreement and the attached Exhibits. Further, Trustee represents and certifies that no Data Trust Member or Data Trust User shall have access to another Data Trust Member's Tier 1, Tier 2 or Tier 3 data in its raw form without express written or electronic approval by the Data Trust Member owning or stewarding over the data.
- E. Trustee will ensure that no Tier 1, Tier 2, or Tier 3 data in its raw form will be included in any published data. During the implementation of Projects and Allowable Uses, Trustee, Data Trust Members, and approved Data Trust Users may develop aggregate data that qualifies for Tier 0 classification as defined by the privacy and anonymization criteria adopted by the Data Governance Council. Such aggregate data may be published in accordance with all other Tier 0 data, as determined by the Data Governance Council. However, prior to any such release, Data Trust Members that own data used in the creation of aggregate data shall be able to review the aggregate data to verify that no Tier 1, Tier 2, Tier 3 or Tier 4 data is revealed.
- F. The Trustee will register and make available all approved Data Trust Users and proposals as directed by the Data Governance Council.

V. APPROVED USES

- A. Academic research is an approved use of the Trust-managed Data Resources. The Trustee shall make available a secure Data Trust Access Hub ("Access Hub") for access by approved Data Trust Users and put in place a process for certifying access to Trust-managed Data Resources through the Access Hub.
- B. Data Trust Users or Data Trust Members may submit a proposal for the use of Trust-managed Data Resources that requires access to one or more Data Trust Member's Tier 1, Tier 2, or Tier 3 data. This proposal must be submitted in writing to the Trustee. Access to Tier 1, Tier 2 or Tier 3 data will only be provided if the proposal is approved by the Trustee and by the Data Trust Member(s) whose data will be accessed. Data Trust Members will retain the right to opt out of the use of their data in any particular project at any time.
- C. Data Trust Users will be required to execute a separate agreement with the Trustee that stipulates the permissions, use, and analyses approved, including timeline and publications. Further, the Trustee must obtain written or electronic consent from Data Trust Member that their Tier 1, Tier 2 or Tier 3 data is authorized for use by such Data Trust User and Data Trust Member may notify Trustee at any time to revoke such Data Trust User's access to the Tier 1, Tier 2 or Tier 3 data. The Trustee will update the Exhibits of this agreement to reflect approved uses and specifications for The Data Trust User's data access.
- D. Prior to being approved for access and use of Data Trust Member-Contributed Data Resources, Data Trust Users shall sign an agreement which covers the use of the Access Hub, allowable use of data provided via the Access Hub, Data Trust User's obligations to Data Trust Members, ethical guidelines, reporting of accidental misuse, and research review prior to publication. The agreement must be signed by the Trustee prior to the Data Trust User obtaining access to the Data Trust Member-Contributed Data Resources.
- E. If applicable, Data Trust Users shall be required to complete relevant Institutional Review Board approval prior to approval for access and use of Trust-managed Data Resources.
- F. The Data Governance Council will periodically review and approve through unanimous vote categories of allowable uses of Tier 1, Tier 2 and Tier 3 data by Data Trust Users along with their associated responsibilities and restrictions.

VI. PROPRIETARY RIGHTS

- A. Data Trust Member shall maintain ownership over any methodologies and code developed using only its own data, except for the code, software, or algorithms developed by the Trustee specific to Data Trust Member-Contributed Data Resources necessary to support and maintain the Trust and approved Projects and Uses.
- B. To the extent practicable, Trustee will release all software and algorithms developed or managed under Projects and Uses, as described in Exhibit A attached to this document, on behalf of the Trust as open source software unless otherwise determined by a vote of the Data Governance Council. In the event such software cannot be made available as open source software due to technical or other limitations, Trustee shall grant Data Trust Member a non-exclusive, royalty-free license to use the software for the purposes set forth in Exhibit A. Notwithstanding anything to the contrary, Trustee is not required to license or incorporate anything into software that Trustee reasonably believes would infringe another Data Trust Member's intellectual property rights or that Trustee is not authorized to license.
- C. Approved Data Trust Users shall maintain ownership over any methodologies developed during the course of their approved Projects and Uses, unless otherwise agreed on by all Parties.
- D. All developments, discoveries, inventions, improvements, and modifications (whether or not patentable) conceived and reduced to practice in carrying out Projects and Uses conducted under this Agreement (the "Inventions") will be promptly disclosed by each Party to the other Party. Inventions made solely by employees, agents, consultants, independent contractors or other representatives of the Trustee will be solely owned by the Commonwealth of Virginia. Inventions made solely by employees, agents, consultants, or other representatives of Data Trust Member, will be owned solely by Data Trust Member, or if the Data Trust Member is a state agency, then by the Commonwealth of Virginia. Inventions made jointly by employees, agents, consultants, independent contractors or other representatives of the Trustee and/or employees, agents, consultants, or other representatives of Data Trust Member will be owned jointly by the jointly contributing Parties.
- E. This Agreement does not transfer from one Party to the other any intellectual property rights that existed prior to this Agreement or that are created independently of this Agreement.

VII. LIABILITY

A. Each Party represents and certifies that:

1. It has the right and necessary corporate authority to enter into this Agreement.
2. It has obtained all necessary consents, waivers, and permission to fulfil the purposes contemplated by this Agreement. For the avoidance of doubt, Data Trust Member shall be solely responsible for obtaining all necessary consents and otherwise complying with applicable law in transmitting Tier 0, Tier 1, Tier 2 and Tier 3 Data to the Trustee and to permit the Trustee to perform its obligations pursuant to this Agreement.
3. ANY DERIVED DATA, AGGREGATE DATA, TRUST-OWNED DATA, AND RESEARCH OUTPUTS CREATED UNDER THIS AGREEMENT ARE PROVIDED "AS IS". THE TRUSTEE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE WORK OR PRODUCTS OF WORK CREATED UNDER THIS AGREEMENT, INCLUDING ANY EXPRESS OR IMPLIED WARRANTIES OF NON-INFRINGEMENT, OWNERSHIP, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OF THE DATA GENERATION, RESEARCH OR ANY INVENTION OR PRODUCT. ANY DATA TRUST MEMBER-CONTRIBUTED DATA RESOURCES ARE PROVIDED "AS IS". THE DATA TRUST MEMBER MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE ACCURACY, COMPLETENESS, OR RELIABILITY OF DATA TRUST MEMBER-CONTRIBUTED DATA RESOURCES UNDER THIS AGREEMENT, INCLUDING ANY EXPRESS OR IMPLIED WARRANTIES OF NON-INFRINGEMENT, OWNERSHIP, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OF THE DATA GENERATION, RESEARCH OR ANY INVENTION OR PRODUCT.
4. Each party shall be responsible for its negligent acts or omissions and the negligent acts or omissions of its officers, directors, employees, and affiliates to the extent allowed by law. Except with respect to: (i) either Party's breach of applicable law, or (ii) any Party's negligence or willful misconduct, no Party shall be liable hereunder for consequential, exemplary, or punitive damages (including lost profits or savings)

VIII. CONFIDENTIALITY

- A. In performance of this Agreement the Parties may disclose to each other, either in writing or orally, information which the disclosing Party deems to be a trade secret, proprietary and/or confidential (hereinafter, "Confidential Information") and not shared with the Data Trust, but may be necessary for the Trustee to perform its duties.
- B. Confidential Information shall be maintained in confidence during the term of this Agreement and for a period of three (3) years following the termination of this Agreement, except to the extent that it is required to be disclosed by law. After such time, Confidential Information shall be destroyed.
- C. Confidential Information does not include information which is (i) known by the Trustee or other Data Trust Members prior to disclosure to them; (ii) generally available to the public other than as a result of breach of this Agreement; (iii) made available to the Trustee or other Data Trust Members by any independent third party who has the right to disclose the information; (iv) information that is published; (v) is independently developed by the Trustee or other Data Trust Members; or (vi) is required to be disclosed by law or a court of competent jurisdiction.
- D. In such a case where legal notice of disclosure is received, the Trustee will advise the Data Trust Member prior to disclosure so that the Data Trust Member will have an opportunity to seek a protective order or other appropriate relief.
- E. No Party shall disclose Confidential Information to any third party, and each Party shall keep strictly confidential all Confidential Information of the other. Using reasonable means, each Party shall protect the confidentiality thereof with at least the same level of effort that it employs to protect the confidentiality of its own proprietary and confidential information of like importance. The Trustee, when receiving any such Confidential Information of a Data Trust Member may, however, disclose any portion of the Confidential Information of the Data Trust Member to such representatives of the Trustee as are engaged in a use permitted by this Agreement and have a need to know such portion, provided that representatives: (i) are directed to treat such Confidential Information confidentially and not to use such Confidential Information other than as permitted hereby or subsequently approved by Data Trust Member, and (ii) are subject to a legal duty to maintain the confidentiality thereof. No receiving Party shall use the Confidential Information of a disclosing Party except solely to the extent necessary in and during the performance of this Agreement, as expressly licensed hereunder, or subsequently through electronically approved updates to this Agreement by a disclosing party. The receiving Party shall be responsible for any improper use or disclosure of any of the disclosing Party's Confidential Information by any of the receiving Party's current or former representatives.

IX. PUBLICATION

- A. Subject to the conditions herein, Data Trust Users may be permitted to, consistent with academic standards, publish product(s) produced under this Agreement, provided such publication does not disclose Confidential Information, Tier 1, Tier 2, Tier 3, or Tier 4 Data of Data Trust Members. Data Trust Users shall not publish any product(s), Confidential Information or any data of the Data Trust without the express written approval of the Trustee.
- B. Data Trust Users shall be required to agree that, prior to submission of all product(s) describing any results for publication, the Data Trust User will submit the product(s) to the Trustee for review. The Trustee shall then forward to all Data Trust Members, the submitted product(s) and shall allow Data Trust Members thirty (30) days to determine whether: the product(s) contain(s) Confidential Information; the product(s) contain(s) Tiers 1-4 Data; and whether a patent application or other intellectual property protection should be sought prior to publication in order to protect the Data Trust Member's proprietary interests in any product or invention developed in connection with the approved Project.
- C. In the event that a Data Trust Member notifies the Trustee pursuant to Section IX(B) that the product(s) contain(s) Confidential Information or Tiers 1-4 Data, then the Trustee shall require the Data Trust User to remove Confidential Information or Tiers 1-4 Data from the product(s). The Trustee shall also require the Data Trust User to resubmit the product(s) for review pursuant to Section IX.
- D. In the event that a patent application or other intellectual property protection is desired, then the Trustee, with reasonable justification, shall withhold approval of such publication to obtain patent or other intellectual property protection. Neither party shall use the name of the other party, or the name(s) of the other party's employees, logos, trademarks or other identifiers, without the prior written consent of the other party, except that the Trustee may list Data Trust Member as a member on a public site and Data Trust User may list the Trust as a resource on any published product(s) after final approval.

X. ETHICAL USE

- A. Parties agree to abide by a set of ethical principles around data trust creation, management, and use (Exhibit E).
- B. Ethical commitments enumerated in this Agreement may be updated through unanimous vote by the Data Governance Council. Any approved changes or additions by the Data Governance Council are applicable to all Data Trust Members, Trustee, and Data Trust Users within thirty (30) days of modification. Trustee must update the ethical commitments enumerated in this Agreement within 7 days of Data Governance Council approval and send electronic notice to all Data Trust Members and Data Trust Users of the changes to the ethical obligations within 14 days of approval.

XI. TERM AND TERMINATION

- A. The initial term of this Agreement shall commence on the Effective Date and will remain in effect for four (4) years thereafter unless otherwise modified by mutual agreement. Any party may terminate their involvement in this Agreement without cause upon thirty (30) days' prior written notice to the other party. Termination of involvement in this agreement by any party shall not affect the involvement of any other party in this agreement. Upon termination Data Trust Member may elect to have the Trustee destroy their Tier 0, Tier 1, Tier 2, and Tier 3 Data. Data Trust Member may also renew the Agreement and Trust Membership for an additional four (4) year period at any time via written or electronic communication with Trustee. Trustee will retain a registry of the expiration date of the agreement for all Data Trust Members.

XII. MISCELLANEOUS.

- A. Amendments. Except as otherwise expressly provided herein, this Agreement may not be modified, amended, or altered in any way except by a written agreement signed by the Parties or electronic consent provided by Parties.
- B. Assignment. Neither Party may assign this Agreement or delegate any of its duties, in whole or in part, unless required to by law.
- C. Counterparts. This Agreement may be executed in multiple counterparts, each of which shall be deemed an original and all of which together shall be deemed the same agreement.
- D. Force Majeure. Neither Party shall be liable for any failure or delay in performing its obligations under this Agreement, or for any loss or damage resulting therefrom, due to acts of God, the public enemy, terrorist activities, riots, fires, and similar causes beyond such Party's control.
- E. Governing Law. This Agreement is governed by and will be construed in accordance with the laws of the Commonwealth of Virginia without regard to that body of law controlling choice of law. Any and all litigation relating to this Agreement must be brought in the circuit courts of the Commonwealth of Virginia.

- F. **Publicity.** Neither Party shall make reference to the other Party in a press release or any other written statement in connection with the Project without the other Party's prior consent, which consent shall not be unreasonably withheld. If there is no notice or disapproval within 5 business days after delivery to the other party for its review, the material shall be deemed approved. Notwithstanding the foregoing, Trustee shall be permitted to use Data Trust Member's name in a list of Data Trust Members that may also include a brief description of the Trust goals and priorities.
- G. **Severability.** Invalidity of any term of this Agreement, in whole or in part, shall not affect the validity of any other term. The Data Trust Member and Trustee further agree that in the event such provision is an essential part of this Agreement, they shall immediately begin negotiations for a suitable replacement provision.
- H. **Survival.** Any provisions of this Agreement regarding Proprietary Rights and Confidentiality, Liability, Indemnification and Publication shall survive the expiration or termination of this Agreement.
- I. **Entire Agreement.** The following Exhibits, including all subparts thereof, are attached to this Agreement and are made a part of this Agreement for all purposes:
 - Exhibit A - Approved Uses and Projects
 - Exhibit B – Data Trust Member-Contributed Data Resources
 - Exhibit C – Approved Users, Uses and Access Tier (Data Trust Users)
 - Exhibit D – Technical Infrastructure
 - Exhibit E – Ethical Principles
 - Exhibit F – Additional Conditions, Memoranda of Understanding, or Data Use Agreements Governing Data Trust Member-Contributed Data Resources

This Agreement and its Exhibits constitute the entire agreement between the Parties and supersede any and all previous representations, understandings, discussions or agreements between the Parties as to the subject matter hereof. The Parties each acknowledge that it has had the opportunity to review this Agreement and to obtain appropriate legal review if it so chose.

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement in duplicate by proper persons thereunto duly authorized.

Virginia Department of XXX [Data Trust Member]	Commonwealth of Virginia Chief Data Officer [Trustee]
By:	By:
Name:	Name: Carlos Rivero
Title:	Title: Chief Data Officer
Date:	Date: 29 March 2020

EXHIBIT A - APPROVED USES AND PROJECTS

An electronic registry of EXHIBIT A Approved Uses and Projects is maintained and updated at:

[insert DataSAGE Project Registry URL]

ORGANIZATION	
PRINCIPAL PROJECT OFFICER	
PROJECT TITLE	
PROJECT PURPOSE	
INTENDED USE	
WHY DOES THE PROJECT REQUIRE TIER 1-3 DATA?	
HOW DOES THIS PROJECT ALIGN WITH COMMONWEALTH OF VIRGINIA GOALS AND OBJECTIVES?	
PROJECT STAKEHOLDERS	
ANTICIPATED RESULTS	

EXHIBIT B - DATA TRUST MEMBER-CONTRIBUTED DATA RESOURCES

An electronic registry of EXHIBIT B Data Trust Member-Contributed Data Resources is maintained and updated at:

<https://metadata.cdo.virginia.gov>

Update Frequency: [HOURLY/DAILY/WEEKLY/MONTHLY]

DATA_ASSET_NAME	DESCRIPTION
DATA ELEMENT 1	
DATA ELEMENT N	

EXHIBIT C - APPROVED USERS, USES, AND ACCESS TIER (DATA TRUST USERS)

An electronic registry of EXHIBIT C Approved Users, Uses, and Access Tier (Data Trust Users) is maintained and updated at:

[insert DataSAGE User Registry URL]

TEAM_MEMBER_NAME	
PROJECT_TITLE	
POSITION	
US_CITIZEN	
NDA_SIGNED	
CRIMINAL_BACKGROUND_CHECK_PERFORMED	
CRIMINAL_BACKGROUND_CHECK_DATE	

EXHIBIT D – TECHNICAL INFRASTRUCTURE

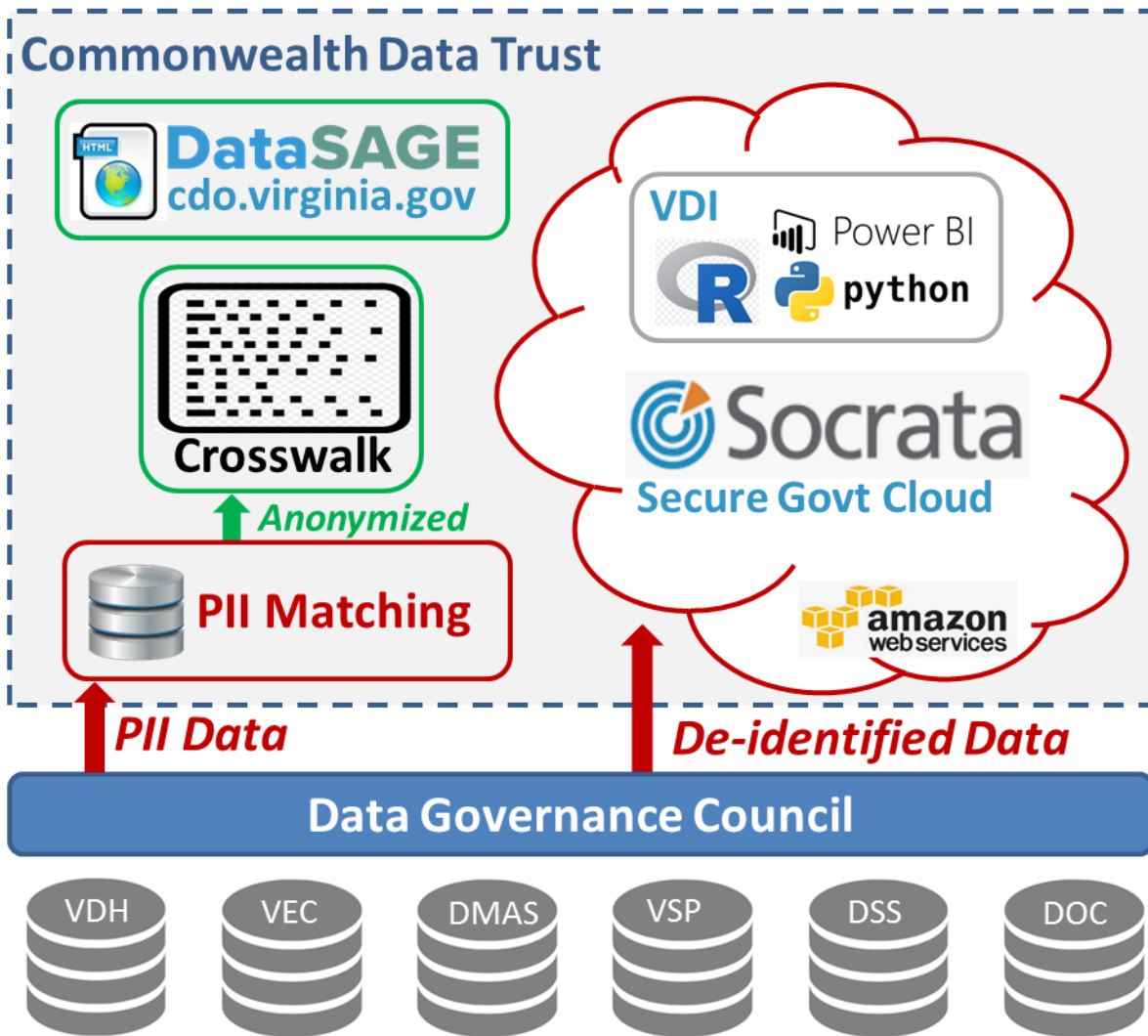


EXHIBIT E – ETHICAL PRINCIPLES

All individuals participating in the data trust or utilizing data trust resources, including Data Governance Council Representatives, Data Trust Members, Data Trust Users, Executive Data Board Members, Trustee, or any other individual utilizing data trust resources shall adhere to the following ethical principles when handling Data provided to the Trust as detailed in Exhibit B for the allowable uses and projects outlined in Exhibit A:

A. Respect

1. Parties shall consider whether the insights gleaned from use of the data could unfairly limit an individual's or a community's opportunities
2. Parties shall not use data in a way that could stigmatize or portray demographic groups, cultures, or communities in terms of deficit.
3. Parties assessing the ethical benefits and harms of data use should conduct assessments from the perspective of the individuals, groups, or communities to whom the data relate.
4. Parties shall actively work to mitigate the potential harm to individuals and communities that could occur from use of the data.
5. Parties shall actively work to understand, mitigate, and communicate the presence of bias in the data.

B. Privacy

1. Parties shall make every effort to guarantee the security of data, subjects, and algorithms to prevent unauthorized access, disclosure of sensitive information, policy violations, tampering, or harm to data subjects.
2. Parties shall make every effort to protect anonymous data subjects, and any associated data, against any attempts to reverse-engineer, de-anonymize, or otherwise expose confidential information.

C. Transparency

1. Parties shall work to implement and maintain auditability in all uses of data.
2. Parties shall make every effort to provide mechanisms for tracking the context of collection, methods of consent, the chain of responsibility, and assessments of quality and accuracy of the data, where applicable.
3. Parties shall establish consistent review practices for data and process auditability.
4. Parties shall provide sufficient context and documentation to enable other trained parties or practitioners to evaluate the use of data.
5. Parties shall ensure that metadata acknowledges the provenance and purpose and any limitations or obligations in secondary use inclusive of issues of consent.

D. Openness

1. Parties shall work to include representation from relevant data subjects or communities, where applicable
2. Parties shall work to foster diversity by ensuring inclusion of a variety of communities and philosophies when working with data.
3. Parties shall engage in responsible communication with stakeholders of data resources, considering and providing clear opportunities for feedback from all stakeholders.

E. Integrity

1. Parties shall use data in ways that are consistent with the intentions and understanding of the disclosing party.
2. Parties shall make every effort to ensure that future use of the data conforms with the intentions and understanding of the disclosing party.
3. Parties shall acknowledge and disclose caveats and limitations to the process and outputs.

EXHIBIT F

ADDITIONAL CONDITIONS, MEMORANDA OF UNDERSTANDING, OR DATA USE AGREEMENTS GOVERNING DATA TRUST MEMBER-CONTRIBUTED DATA RESOURCES

[Data Trust Members should include copies of any existing Memoranda of Understanding, Agency Supplied Terms, or Data Use Agreements governing Data Trust Member-Contributed Data Resources between Data Trust Members and/or Trustee]

An electronic version of EXHIBIT F is maintained and updated at:

[insert MOU/DUA Registry URL]